REMARKS

Applicant respectfully requests reconsideration of the rejected claims. Claims 1, 4-8, 11-13, 15-21, 23-30, 32, 35-39, 42-44 remain in the application. No claims have been amended, canceled, or added.

Claim Rejections under 35 U.S.C. § 101

Claims 1, 4-6, 8, 13, 15-17, 20, 32, 35-37, and 39 have been rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Claims 1, 8, 13, 32, and 39

The Examiner states that Claims 1, 8, 13, and 32 recite no practical result, but an intermediate operation. (Examiner did not discuss 39 and thus Applicant assumes that the Examiner meant to include 39 as well). The claims explicitly requiring the processing of a data cipher. For instance, Claims 1 and 32 recites, in part, "processing the data cipher operation..." Also, Claims 8 and 39 recites, in part, "receiving a request to perform for data ciphering...and processing the request..." And finally, Claim 13 recites, in part, "a processing unit coupled to the memory, the processing unit to execute a data ciphering operation..." Different ciphers have been developed to allow for secure communications between remote systems using different security protocols. (Application as filed; paragraph 0005). Current approaches for RC4 are limited in their execution speed due to the bottlenecking that occurs while accessing the S-box. (Application as filed; paragraph 0006). Furthermore, the invention is not limited to RC4, but can be used in different data

ciphers, e.g. AES and DES. (Application as filed; paragraph 0039). One benefit of the claimed invention is to provide faster execution of data ciphering by reducing the bottleneck of memory access. Therefore, Claims 1, 8, 13, 32, and 39 provide for the processing of a data ciphering operation which yields faster encryption of plaintext to ciphertext (and ciphertext to plaintext) by reducing the bottleneck during memory access. (Application as filed; paragraphs 0039, 0090). Therefore, Applicant respectfully submits that Claims 1, 8, 13, 32, and 39 do recite a practical result, and thus the rejection is overcome. If the Examiner wishes to maintain the rejection, Applicant requests an interview at which the Applicant will present proposed language to overcome the rejection and still maintain the breadth of the Applicant's invention.

Claims 2-6, 15-17, 20, 35-37, and 42-44

Applicants respectfully submit that Claims 2-6, 15-17, 20, 35-37, and 42-44 are dependent directly or indirectly on Claims 1, 8, 13, 32, or 30; and thus, include the same limitations as one of the independent Claims 1, 8, 13, 32, and 39. As such, the rejection for Claims 2-6, 15-17, 20, 35-37, and 42-44 are overcome for at least the same reasons discussed for Claims 1, 8, 13, 32, and 39 above.

Claims 7, and 11-12, 18-19, 38, and 42-44

Claims 7, and 11-12, 18-19, 38, and 42-44 are objected to, but would overcome the 101 issues if rewritten to include all of the limitations of the base claim and any intervening claims.

Applicants respectfully submit that Claims 7, and 11-12, 18-19, 38, and 42-44 are dependent directly or indirectly on Claims 1, 8, 13, 32, or 30; and thus, include the same limitations as one of the independent Claims 1, 8, 13, 32, and 39. As such, the rejection for Claims 7, and 11-12, 18-19, 38, and 42-44 are overcome for at least the same reasons discussed for Claims 1, 8, 13, 32, and 39 above.

The Alleged System Described in Paragraphs 5-7 of the Office Action's "Response to Amendment" Section

Applicant would first like to address the Examiner's "Response to Amendment" on page 2 of the Office Action in an effort to assist in the understanding of the claimed invention and the Applicant's response to this rejection. In particular, the Applicant would like to address paragraphs 5, 6, and 7. No reference has been provided for these paragraphs; however, it appears that there is no rejection given on the assertions in these paragraphs. As such, applicant will only briefly touch on these statements. For convenience, paragraphs 5-7 have been reproduced below:

> 5. The instant application applies the technique of speculative execution, which combines dynamic scheduling with branch prediction, and was conventional and well known technique at the time the invention was made, to the encryption field.
>
> 6. Speculative execution as someone of ordinary skill in the art would promptly recognize, calls for re-executing the instructions should a miss prediction occur.
>
> 7. The fact that the instant application recites cipher operations/instructions is not persuasive since the processors use speculative execution techniques to 'execute instructions' regardless of what type of instructions. Using a processor that uses speculative execution to implement a conventional and well known encryption algorithm is not patentably different from a processor that uses speculative execution.

The specification describes the generation of two portions of ciphertext wherein a speculative load associated with the second portion of ciphertext is performed prior to the store associated with the prior portion of ciphertext, from which recovery (through a subsequent re-execution) is necessary if the speculative load associated with the later portion of ciphertext conflicts with the store associated with the prior portion of ciphertext. For example, Claims 1 specifically requires the generation of two portions of ciphertext in a single iteration through the use of a speculative load from which recovery (through re-execution on a different iteration) is necessary if the speculative load of the later portion of ciphertext conflicts with the store of the prior portion of ciphertext.

It should be noted that a processor performing speculative execution through branch prediction is not equivalent to performing a speculative load hoping there will not be a collision with a store, and then recovering as necessary when the hope turns out not to be true. Rather, branch prediction guesses whether a branch will be taken or not, and then backs up execution of the instruction stream to the point of the branch when it is incorrect. The specification describes performing the speculative load (there is no conditional branch that makes the speculative load speculative) prior to the store, and in some claims during the same iteration, of a prior portion of ciphertext, and then recovering if there was a collision between the speculative load and the store of the prior portion of ciphertext. As discussed below, the claimed invention is also different from the speculation performed by Goldberg.

Claim Rejections under 35 U.S.C. §103(a)

Claims 1, 4-8, 11-13, 15-21, 23-30, 32, 35-39, 42-44 have been rejected under 35 USC §103(a) as being unpatentable over Goldberg et al. (NPL "Architectural Consideration for Cryptanalytic Hardware", hereinafter Goldberg).

Applicant points out that Goldberg's teaching is performing a **type of speculative execution in hardware where all possibilities are performed and the correct output is chosen**. Goldberg states, "We do speculative execution with four functional cells; each cell computes the output of the 6-to-1 function under a speculative assumption about the 2 control bits. As there are four possible values of the control bits, the four functional cells enumerate all possibilities. At the same time the functional cells are computing their 4-to-1 function, a multiplexor unit concurrently selects one of the functional cells." (Goldberg; page 9, paragraph 6). It should be noted that all of the inputs are the same to each of the speculative execution cells. (Goldberg, page 10, Figure 3). There are no load/store conflicts and there is no speculative loading associated with a second portion of ciphertext that is occurring prior to the store associated with a prior portion of ciphertext. Further, there is no concept of recovery. In addition, there is no concept of generating two portions of ciphertext in a single iteration when there is not conflict, and only one where there is a conflict.

Claims 1, 8, 32, and 39

Independent Claims 1, 8, 32, and 39 include language for 1) speculative loading associated with a second portion of ciphertext that is occurring prior to the

store associated with a prior portion of ciphertext, and 2) the generation of two portions of ciphertext in a single iteration when there is not conflict, and only one where there is conflict (requiring re-execution in an subsequent iteration). As discussed above, Goldberg fails to describe or suggest this limitation and therefore does not render Claims 1, 8, 32, and 39 obvious.

Claims 4-7, 11-12, 35-38, and 42-44

Applicants respectfully submit that Claims 4-7 are dependent directly or indirectly on Claim 1, thus include the same limitations as Claim 1. As such, Claims 4-7 are patentable for at least the same reasons as Claim 1.

Applicants respectfully submit that Claims 11-12 are dependent directly or indirectly on Claim 8, thus include the same limitations as Claim 8. As such, Claims 11-12 are patentable for at least the same reasons as Claim 8.

Applicants respectfully submit that Claims 35-38 are dependent directly or indirectly on Claim 32, thus include the same limitations as Claim 32. As such, Claims 35-38 are patentable for at least the same reasons as Claim 32.

Applicants respectfully submit that Claims 42-44 are dependent directly or indirectly on Claim 39, thus include the same limitations as Claim 39. As such, Claims 42-44 are patentable for at least the same reasons as Claim 39.

Claims 13, 21, 28

Independent Claims 13, 21, 28 include language for 1) an access (or read) for data ciphering a second portion of plaintext that occurs prior to the completion of the

swap for data ciphering a prior portion of plaintext, and 2) data ciphering a second portion of plaintext when the data being swapped (from data ciphering a prior portion of plaintext) does not equal the data being accessed (or read) for data ciphering the second portion of plaintext. As discussed above, Goldberg fails to describe or suggest this limitation and therefore does not render Claims 13, 21, 28 obvious.

Claims 15-20, 23-24, and 29-30

Applicants respectfully submit that Claims 15-20 are dependent directly or indirectly on Claim 13, thus include the same limitations as Claim 13. As such, Claims 15-20 are patentable for at least the same reasons as Claim 13.

Applicants respectfully submit that Claims 23-24 are dependent directly or indirectly on Claim 21, thus include the same limitations as Claim 21. As such, Claims 23-24 are patentable for at least the same reasons as Claim 21.

Applicants respectfully submit that Claims 29-30 are dependent directly or indirectly on Claim 28, thus include the same limitations as Claim 28. As such, Claims 29-30 are patentable for at least the same reasons as Claim 28.

Claim 25

Independent Claim 25 describes an RC4 state machine which generates "a subset of said plurality of output text blocks . . . as a result of repeating the same sequence of states." During these "sequence of states data is speculatively read...as part of the generation of a next one of said plurality of output text blocks prior to a write...completing as part of generation of a current one of said plurality of

output text blocks." (Emphasis added). As discussed above, Goldberg fails to describe or suggest this limitation and therefore does not render Claim 25 obvious.

Claims 26-27

Applicants respectfully submit that Claims 26-27 are dependent directly or indirectly on Claim 25, thus include the same limitations as Claim 25. As such, Claims 26-27 are patentable for at least the same reasons as Claim 25.

Furthermore, Applicant points out that one benefit of the claimed invention is reducing the bottleneck of memory access. (Application as filed; paragraph 0090 and 0006). Goldberg (nor the asserted system of paragraph 5-7 of the "Response to Amendment" in the Office Action) directly address this issue. Specifically, in Goldberg, all of the inputs are to each speculative execution cell, so there is no reduction of bottlenecking to memory access through speculative loads and recovery described. The system of paragraph 5-7 does not address this issue either.

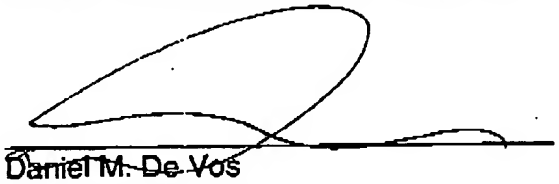
Therefore, Applicant respectfully submits that Goldberg (nor the system in paragraph 5-7) render Claims 1, 4-8, 11-13, 15-21, 23-30, 32, 35-39, 42-44 obvious, and thus the claims are in a condition for allowance.

RECEIVED
CENTRAL FAX CENTER
JAN 0 8 2007

Conclusion

Applicant respectfully submits that the rejections have been overcome by the remarks. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims allowed. If the allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact the undersigned at (408) 720-8300. If there are any additional charges, please charge our Deposit Account No. 02–2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP



Dated: January 8, 2007

Daniel M. De Vos
Registration No. 37,813

Customer No. 08791
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030
(408) 720-8300

PAGE 25/25 * RCVD AT 1/8/2007 6:48:51 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/18 * DNIS:2738300 * CSID:408 720 9397 * DURATION (mm-ss):07-08